

Robo de información personal usando mensajes de texto

SMISHING

Mensaje para el consumidor

¿QUÉ ES 'SMISHING'?

SMiShing (pronunciado “smiching”) es una amenaza electrónica que coge como blanco los usuarios de teléfonos celulares y aparatos móviles. Semajante a las estafas de los correos electrónicos de phishing, estafadores usan mensajes de textos con la intención de que los clientes de los inalámbricos divulguen su información personal, financiera o para que descarguen programas que terminan dañando a la computadora.

El término SMiShing está derivado de la combinación de los términos SMS (Short Message Service) la tecnología usada para mandar mensajes de textos, y phishing.

En un clásico ejemplo de una estafa de SMiShing, un cliente de un inalámbrico recibe un mensaje que le pide atención inmediata y le dice que vaya a un sitio web especial o que llame a cierto número de teléfono para resolver el problema. El mensaje puede parecer que viene de la institución financiera del cliente, su servicio de utilidad pública o cualquier otra bien conocida fuente, e indica que la cuenta ha sido suspendida, desactivada, cerrada, etc., y provee un número de teléfono para que llame para re activarla.

El peligro está en clientes que no sospechan nada y pueden llamar al número de teléfono, y proveer información personal, el número de cuenta de banco, el número de Seguro Social, su identidad como usuario, su contraseña y el Número Personal de Identificación (PIN) a una persona o a un servicio automático pensando que es su institución financiera. En realidad, esta información se la da al estafador que la puede usar para acceder a la cuenta del cliente o para abrir una cuenta nueva sin que éste lo sepa.

SEÑALES COMUNES DE LA ESTAFA

Aunque los mensajes de SMiShing están diseñados para que parezcan igual a los mensajes de texto verdaderos, tienen algunas señales en común que puede reconocer:

- La urgencia para que el cliente tome acción inmediata;
- Mencionar que algo negativo pasará si no actúa;
- La falta de un número de teléfono indicando el origen del mensaje.

NO RESPONDA a ningún mensaje que le parezca sospechoso, y que puede ser una estafa SMiShing. **NO RESPONDA CON UN TEXTO**. Si le proveen un número **NO LLAME** a éste. En vez, póngase en contacto directamente con su institución financiera o servicio público de utilidad y pregúntele si en realidad hay un problema con su cuenta.



800-242-5846 • www.NJConsumerAffairs.gov

Office of the Attorney General



New Jersey Division of
**Consumer
Affairs**